Information Commissioner's Office
Internal Audit Plan 2016-17

June 2016

Contents Page

Appendices

This document is confidential and is intended for use by the management and Directors of the Information Commissioners Office only. It forms part of our continuing dialogue with you. It should not be made available, in whole or in part, to any third party without our written prior consent. We do not accept responsibility for any reliance that third parties may place upon the report. Any third party relying on this report does so entirely at its own risk. We accept no liability to any third party for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however, such loss or damage is caused.

It is the responsibility of Information Commissioners Office's management to ensure that there are adequate risk management, governance and control arrangements.

© 2016 Grant Thornton UK LLP. All rights reserved

1 Developing the Internal Audit Plan

1.1 Overview of our internal audit approach

Our role as internal auditor to an executive NDPB is to provide an independent and objective opinion to the Management Board on the adequacy and effectiveness of its risk management, control and governance processes. Our approach, as set out in the firm's Internal Audit Manual, is to help the organisation to accomplish its objectives by bringing a systematic, disciplined approach to our evaluation and to help improve the effectiveness of its risk management, control and governance processes.

Our approach complies with best professional practice, in particular, the standards for internal audit promulgated by HM Treasury (Public Sector Internal Audit Standards, PSIAS), and the Institute of Internal Auditors' guidance on risk-based internal auditing. We also comply in all material respects with other Government guidance applicable to executive NDPBs.

1.2 Our Internal Audit Plan for the Information Commissioner's Office

Our proposed 2015-16 Internal Audit Plan has been prepared based upon:

- your latest risk register;
- our understanding of your key challenges and objectives; and
- discussions with management.

In taking this approach, and in compliance with PSIAS requirements, the Internal Audit Plan is developed to enable us to provide distinct assurance to the Management Board and the Information Commissioner (as Accounting Officer) as to the adequacy and effectiveness of the risk management activities and controls in each of the three areas of:

- risk management;
- governance; and
- internal control.

© 2016 Grant Thornton UK LLP. All rights reserved

2 Internal Audit Plan 2016-17

2.1 Reporting outputs

Our Internal Audit Plan will deliver the following reporting outputs to management and the Audit Committee throughout the year:

- audit planning briefs;
- assignment reports;
- progress reports to the Audit Committee; and
- Internal Audit Annual Report.

Audit planning briefs

Every internal audit assignment will have audit planning brief that must be agreed with you before we begin any audit fieldwork. As well as capturing the background of the audit area, the scope of the review and the approach we will take, it also identifies key members of your staff who we will engage with and a timetable for fieldwork and reporting. It is prepared following detailed planning meeting(s) with your nominated client leads, and typically takes place six to eight weeks before our fieldwork begins. Each brief is subject to our usual quality assurance arrangements, i.e. is reviewed by the engagement manager and partner before it is issued to you for approval.

Assignment reports

We produce a separate assignment report for every review in the Plan. It has two core sections:

- an Executive Summary of the scope, key findings, best practice and our rating for the review area
- a schedule of our detailed findings, including our agreed audit recommendations and your management response.

We issue the assignment report in draft for your consideration and response within 15 days of completing our fieldwork. It is subject to our internal quality assurance review processes before it is issued in draft.

Progress reports to management and the Audit Committee

We issue a progress report to support to each meeting of the Audit Committee that shows the current status of each assignment in the Plan and highlights any emerging risks that may warrant a variation to the Plan.

Internal Audit Annual Report

Our Internal Audit Annual Report will contain our annual opinion on risk management, governance and internal control. It will summarise:

- the opinion and level of recommendations for each audit assignment;
- how each review has informed the annual opinion we give, and the reasons behind any qualification we may give;
- progress made in addressing any significant findings; and
- our performance against agreed performance indicators.

© 2016 Grant Thornton UK LLP. All rights reserved

2.2 Proposed Internal Audit Plan

We identify below the areas agreed for consideration in the Internal Audit Plan, which we will keep under review throughout the year.

Review	Scope	Audit Lead	Budget estimate 2016-17			
			Q1	Q2	Q3	Q4
Reviews for consideration						
Fines recovery	Review the process in place to recover fines issued to organisations that remain unpaid. The review will are cover how unpaid fines are identified, performance measures of fine payment are reported and the success of follow up activities to recover fines to ensure this process is efficient and effective.	Will Simpson	6			
IT service delivery	An IT operational review of the IT services delivered to ICO, considering performance management of suppliers, contract management with Northgate and how the ICO determines whether those services are meeting user needs. The review has been timed to allow any lessons learnt or findings to be considered as part of establishing new IT contacts, expected in October 2016.	Paul Eckersley		7		
GDPR project	Provide assurance over the project to manage the impact of GDPR on the ICO, including governance over the change programme and interactions with other parts of the ICO. The review will include how the ICO have resourced the project and the activity to backfill project members' roles and the recruitment for the new activities as ICO takes responsibility for GDPR.	Will Simpson		8		
Investigations	The review will cover how the ICO manages investigations through communication with stakeholders, the use of frameworks, gathering intelligence and finally reporting on investigations. Where possible, we will benchmark against other regulators management of investigations.	Will Simpson			9	
People Strategy	People are a key part of the ICO and the management have established that the organisation needs to ensure it has "the right people, in the right place at the right time". The review will consider how staff performance is managed across the organisation and that managers are properly prepared to implement performance management to ensure consistency. The review will also consider the progress of recommendations made from the staff performance review in 2015-16.	Will Simpson			8	
Stakeholder engagement	ICO is tasked with communicating key messages on data protection (and in the future data privacy) and access to information. A review will establish how those communications are prepared and published including thought leadership. The focus will be on how strategic activity is determined, agreed and approved, including consideration of the impact of GDPR on these activities. The review will also determine how the target audience is selected and the medium to use. How the ICO measures the success of such communication will also be assessed.	Will Simpson				11.5
Follow Up	Review of the arrangements to capture and implement audit recommendations in a timely manner.	Paul Eckersley				3.5
	Sub-total by quarter		*6*	*15*	*17*	15
Planning, continued liaison, attendance at Audit Committee, annual reporting			8			
TOTAL			**61**			

© 2016 Grant Thornton UK LLP. All rights reserved

2.3 Reviews considered and deferred

The following areas were discussed with management but have been deferred:

Review	Scope	Budget estimate	Reason for deferring
Sharepoint implementation advisory	ICO continue to develop new systems and a replacement is needed for Meridio. The review will provide advice on the implementation options available when using Sharepoint, based upon our experience of other organisation's implementation.	5 days	Have advisors in place
Fee Forecasting	Future work and organisational planning will become more reliant upon the ability of the ICO to forecast its income. The ICO has historically used to a budget model where expenditure could not exceed the budget. However, if the ICO was able to establish the expected income from Registration Fees, the ICO may be able to plan more strategically and hence deliver more services (such as investigations, education programmes, audits). The audit will establish how the ICO established what the income should be from fees and incorporate the process to chase outstanding fee payment.	7 days	Income is meeting organisation's requirements – possible future review

© 2016 Grant Thornton UK LLP. All rights reserved

2.4 Reviews to be considered for future audit plans

Review	Scope	Budget estimate	
		Audit year	
		2017-18	2018-19
Core processes (may be brought forward into 2016-17 plan)	The new Information Commissioner will be appointed in 2016 and may wish to gain assurance over core processes. The review will cover areas such as Finance, Operations, Corporate Governance (corporate/business planning) and Risk Management. The timing of the review depends on the new Commissioner and may need to be brought forward into the current audit plan.	8-10	
GDPR implementation	General Data Protection Regulation is expected to be finalised in 2016 and individual countries have until 2018 to implement the regulation. The ICO is establishing a programme of work to deal with the impact of GDPR which is planned to be covered in the 2016-17 audit plan. This review is to confirm that the programme has met its objectives.		8-10
Fee income changes/fees forecasting	Future work and organisational planning will become more reliant upon the ability of the ICO to forecast its income. The ICO has historically used to a budget model where expenditure could not exceed the budget. However, if the ICO was able to establish the expected income from Registration Fees, the ICO may be able to plan more strategically and hence deliver more services (such as investigations, education programmes, audits). The audit will establish how the ICO established what the income should be from fees and incorporate the process to chase outstanding fee payment.		7
Recruitment/performance management	Internal Audit reviewed recruitment and staff performance management in 2015-16, identified a number of areas of improvement and this review is to follow up this review. The main focus of the review will be to establish that recruitment and staff performance is meeting the requirements of the ICO, especially as the impact of changes to the ICO role (such as the implementation of GDPR) remain unknown.		7
Sharepoint implementation (Timing is uncertain – dependent on project)	ICO continue to develop new systems and a replacement is needed for Meridio. The review will provide assurance on the implementation of using Sharepoint to replace Meridio.	7?	7?
IT service delivery (post contractual changes)	The contract with Northgate has a break point in 2017, and therefore it is a possibility that the replacement contract, may expire in 2020 and planning for a replacement will need to take place in 2018. The review will focus on the planning for extension or replacement of the contract.		8-10

© 2016 Grant Thornton UK LLP. All rights reserved

Review	Scope	Budget estimate	
		Audit year	
		2017-18	2018-19
Case management system replacement	The case management system is expected to be implemented within ICE, to replace CMEH. The expectation is that the development / implementation in 2017-18. The review will establish that the requirements of the ICO have been captured and that a project / project team is in place to implement the necessary changes.	7	

- Accommodation was considered as an area to review. The next lease break-point for Wycliffe House will be 31 December 2021. The ICO will need to prepare its position two years in advance; ie during 2019/20 and hence the review is not included at this stage.
- Internal compliance & information governance was considered but management concluded that internal ICO experts are best placed to review practice.

© 2016 Grant Thornton UK LLP. All rights reserved

3 Resources and scheduling

3.1 Resources to deliver the Internal Audit Plan

Based upon the assignments proposed in our indicative Plan, the mix of staff we propose to deploy is summarised in the following table.

Grade	Days	Proportion of Time (%)
Business Risk Services		
Partner/Director	4.5	7
Associate Director	10.5	17
IT Audit Manager	5	8
IT Executive	5	8
Executive	29.5	48
Associate	6.5	11
Total	**61**	**100%**

3.2 Previous Internal Audit plans

The table below sets out the assurance provided over the last three years audits and provides information on the previously.

Review	13-14	14-15	15-16
New finance system – benefit realisation			x
Staff recruitment			x
Staff performance management			x
Core operations (post-Eagle)			x
core financial controls			x
Integrated assurance		x	
Business and corporate planning		x	
Preparing for future budget cuts		x	
Project Eagle – lessons learnt		x	
IT support		x	
Finance system project assurance		x	
Governance and decision making	x		
Risk management and horizon scanning	x		
IT service management	x		
IT contract management	x		
Card payment controls in ICE	x		
IT re-procurement lessons learnt	x		
Payroll and pensions	x		
Total of plan (days)	**54**	**39.5**	**47**

© 2016 Grant Thornton UK LLP. All rights reserved

A ICO risk register

We set out below the alignment of what the ICO sees as its key risks (the major risk groups) and the associated Internal Audit reviews.

Risk	Summary information – as per ICO risk register (January 2016)	Covered in 2016-17 Internal Audit Plan	Elements of risk within scope
ICO relevance	The ICO is perceived not to be relevant to the information rights issues of the day by its stakeholders (the public, media, politicians and organisations).	Yes	Stakeholder engagement review – ensure stakeholder needs are being met by focusing resources on the right areas. Investigations – review to establish that investigations are effectively managed and addressing the balance between thorough investigations and maximising the use of resources.
Horizon scanning	The ICO does not identify key information rights trends and issues and we are not successfully scanning the horizon ("looking for trouble").	Yes	GDPR project review – establish how the ICO is preparing for the additional responsibilities for GDPR
Resources	The ICO is not adequately resourced (money, people and IT) or does not make efficient use of its resources.	Yes	IT Service Delivery – ensure that ICO is meeting its user needs from IT services and that the new IT services contract incorporates any findings from the review. People strategy – confirm that the ICO has is addressing resourcing needs and will be ready to take on new responsibilities. Fines recovery – ensure the cost of recovering fines is proportionate to the income from them but also considers the important message of recovering fines.
Change	The ICO is not prepared for change, both internal (the next Commissioner), legislative (the EU DP reforms and the Burn's Commission) and political (government priorities and initiatives).	Yes	GDPR project review – establish how the ICO is preparing for the additional responsibilities for GDPR

© 2016 Grant Thornton UK LLP. All rights reserved

Grant Thornton

An instinct for growth™

www.grant-thornton.co.uk

© 2016 Grant Thornton UK LLP. All rights reserved.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. Please see grant-thornton.co.uk for further details

This publication has been prepared only as a guide. No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication.